Ricardo Edwin More Reaño, Víctor Angel Ancajima-Miñán,
Carmen Lucila Infante Saavedra, Nilo Albert Velásquez-Castillo

Amenaza, riesgo y respuesta

Metodologías de evaluación de riesgos informáticos

ATIK
editorial

Ricardo Edwin More Reaño, Víctor Angel Ancajima-Miñán, Carmen Lucila Infante Saavedra, Nilo Albert Velásquez-Castillo

Amenaza, riesgo y respuesta

Metodologías de evaluación de riesgos informáticos

Atik Editorial

E15D N49-59 y Olivos, San Isidro. Código postal 170515.
Quito, Ecuador
Atik Editorial, es una iniciativa del Centro de Investigaciones CICSHAL y está a cargo del departamento de Comunicación y Difusión Científica.
www.atikeditorial.com

Citar como (APA 7)

More Reaño, R.E., Ancajima-Miñán, V.A., Infante Saavedra, C.L., & Velásquez-Castillo, N.A. (2023). *Amenaza, riesgo y respuesta. Metodologías de evaluación de riesgos informáticos.* Atik Editorial. https://doi.org/10.46652/sjenpy23

Primera Edición: 2023

Ricardo Edwin More Reaño©, Víctor Angel Ancajima-Miñán©, Carmen Lucila Infante Saavedra©, Nilo Albert Velásquez-Castillo©, Atik Editorial©

Amenaza, riesgo y respuesta. Metodologías de evaluación de riesgos informáticos.

Threat, risk and response. IT risk assessment methodologies.

Editorial: Atik Editorial
Materia Dewey: 003 - Sistemas
Clasificación Thema: URD - Privacidad y protección de datos
Público objetivo: Profesional/Académico
Colección: Tecnologías de la Información y las Comunicaciones
Serie: TIC
Soporte: Digital
Formato: Epub (.epub)/PDF (.pdf)
Publicado: 2023-08-31
ISBN: 978-9942-7145-0-3

Disponible para su descarga gratuita en http://atikeditorial.com

ISBN: 978-9942-7145-0-3

El libro retoma y amplía, por un grupo de investigadores, lo mostrado en la tesis "Metodologías de evaluación de riesgos. Informáticos para mejorar la seguridad del área de sistemas de la unidad de gestión educativa local Sullana – Piura, 2016", presentada para la obtención del grado académico de "maestro en Ingeniería de sistemas con mención en tecnología de información y comunicación" en la universidad "Universidad Católica Los Ángeles Chimbote", por "Ricardo Edwin More Reaño ".

Aval de revisión por pares

El presente libro académico fue sometido al proceso de revisión por pares doble ciego. Por lo tanto, la investigación contenida en este libro cuenta con el aval de expertos en el tema, quienes han emitido un juicio objetivo del mismo, confirmando la validez y el nivel del manuscrito, constituyéndose una fuente confiable de consulta.

This academic book has been submitted to a double-blind peer review process. Therefore, the research contained in this book has the endorsement of experts in the field who have made an objective judgment of the same, confirming the validity and level of the manuscript, making it a reliable source of reference.

Autores

Ricardo Edwin More Reaño. Ing. de Sistemas, docente nombrado en Educación Secundaria en la especialidad de Matemática y Física desde el año 1994, docente universitario en Universidad César Vallejo y Universidad Tecnológica del Perú. Actualmente me encuentro realizando actividades de investigación y asesoría en la Universidad. https://orcid.org/0000-0002-6223-4246
Universidad César Vallejo - Perú
remorem@ucvvirtual.edu.pe

Víctor Angel Ancajima-Miñán. Doctor en TIC, Magíster en gestión de TIC e Ingeniero de Sistemas. Docente universitario de pre y posgrado. Auditor y Consultor en TI. Asesor en Investigación Científica. Ponente en temas de TIC, Educación e Investigación. https://orcid.org/0000-0002-3122-4512
Uladech Católica - Perú
vancajimam@gmail.com

Carmen Lucila Infante Saavedra. Ingeniero Industrial con orientación en Sistemas e Informática, Magister en Informática, Doctora en Tecnologías de Información y Comunicación, Doctoranda en Administración de Empresas, Certificada por la Universidad de Liverpool en el curso Adaptación e implementación de cursos virtuales, asesora y jurado de tesis de pregrado y posgrado, miembro del equipo de Semilleros de Investigación y docente principal hace 25 años de la Universidad Nacional de Piura, Facultad de Ingeniería Industrial, Departamento Académico de Ingeniería Informática. Presidenta del Capítulo de Ingenieros Industriales y de Sistemas del Colegio de Ingenieros del Perú del 2022 al 2024. https://orcid.org/0000-0002-5772-8807
Universidad Nacional de Piura - Perú
cinfantes@unp.edu.pe

Nilo Albert Velásquez-Castillo. Doctor en Educación, Magíster en Docencia y Gestión Educativa. Docente universitario de pre y posgrado. Asesor en Gestión del aprendizaje y de procesos de evaluación. Gestor en Acompañamiento Pedagógico Universitario. Ponente en temas de Educación, Investigación. Autor de artículo de investigación.
https://orcid.org/0000-0001-7881-4985
Uladech Católica - Perú
alveca2011@gmail.com

Resumen

El presente libro tiene como objetivo conocer las principales metodologías de evaluación de riesgos informáticos, presentar su aplicación en situación real de una institución pública, proponiendo un plan de mejora de la seguridad del área de sistemas; a fin de garantizar la mejora de la de la seguridad respecto evaluación de riesgos informáticos, se debe tener en cuenta la identificación de los activos para pasar a realizar su valoración, de igual forma las amenazas a las que están expuestos los activos fueron valoradas, lo que permitió determinar las principales salvaguardas según MAGERIT como uno de los principales aportes al campo de la seguridad. Se ha identificado los principales riesgos a los que está expuesta la organización en general. Se ha considerado tener en cuenta lo referente a equipos informáticos, software, datos/información, instalaciones, personal, equipamiento auxiliar como elementos comunes a las diferentes organizaciones tanto privadas como públicas, ya que estas no están ajenas de ser amenazadas o vulneradas tanto por personal externo o interno de estas, lo que amerita medidas de solución inmediata.

Palabras clave: Amenaza; Gestión; Informático; Riesgo; informático.

Abstract

The purpose of this book is to know the main methodologies of computer risk assessment, to present its application in a real situation of a public institution, proposing a plan to improve the security of the systems area; in order to ensure the improvement of security with respect to computer risk assessment, the identification of the assets must be taken into account to proceed to their valuation, likewise the threats to which the assets are exposed were assessed, which allowed to determine the main safeguards according to MAGERIT as one of the main contributions to the field of security. The main risks to which the organization is exposed in general have been identified. It has been considered to take into account computer equipment, software, data/information, facilities, personnel, auxiliary equipment as elements common to the different organizations, both private and public, since these are not exempt from being threatened or violated by external or internal personnel, which merits immediate solution measures.

Keywords: Threat; Management; IT; IT; Risk; IT.

Contenido

Lista de tablas

Listado de gráficos

[Colección Breve]

Amenaza, riesgo y respuesta

Metodologías de evaluación de riesgos informáticos

Serie
TIC

Introducción

Los sistemas de información de las organizaciones tienen multitud de recursos vulnerables ante ataques de seguridad. Por ello, es necesario que desarrollen estrategias y herramientas que sean capaces de identificar y valorar estos recursos y que, a su vez, puedan dar información sobre los ataques y daños que pueden afectarles (Chicano, 2014).

Actualmente las organizaciones, instituciones han evolucionado de forma impresionante en nuestro medio, tanto por la cantidad de recursos humanos que se maneja, cantidad de datos e información así como los recursos económicos que utilizan, por lo tanto esto las ha llevado a implementar diferentes recursos tecnológicos que faciliten el manejo y control de lo descrito anteriormente; pero a la vez ha generado que aparezcan ciertas situaciones de vulnerabilidad, tanto internas como de personas ajenas a las instituciones.

Como lo resalta Escribá y Romero (2013), Uno de los activos más valiosos para cualquier empresa es la información que maneja. La información es el conjunto de datos que da sentido a una empresa, datos que la definen, datos con los que trabaja y datos que, en manos inadecuadas, pueden llevar a la misma a la ruina. Extendiendo este concepto de seguridad al mundo de las telecomunicaciones y la informática, puede entenderse desde dos puntos de vista: seguridad de la información y seguridad informática.

La seguridad de la información es el conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger la integridad, confidencialidad y disponibilidad de la información y la seguridad informática, por su parte, es una rama de la seguridad de la información que trata de proteger la información que utiliza una infraestructura informática y de telecomunicaciones para ser almacenada o transmitida (Escrivá y Romero, 2013).

Las instituciones públicas y privadas de nuestro contexto no han sido ajenas a los cambios globales, pues estas se han desarrollado notablemente; pero al mismo tiempo se han visto amenazadas por que su evolución ha acarreado, lo que tiene que ver con la seguridad de los datos, de la información en su conjunto. En la presente investigación titulada Metodologías de evaluación de riesgos informáticos para mejorar la seguridad del área de sistemas de la UGEL Sullana – Piura, 2016 se realizó la investigación exhaustiva de cada uno de los procesos que se llevan a cabo en el área de sistemas, los mismos que fueron procesados, analizados y comparados con las diferentes metodologías existentes relacionadas a la evaluación de riesgos informáticos.

Por lo expuesto se planteó la siguiente pregunta: ¿La aplicación de metodologías de evaluación de riesgos informáticos permite proponer un plan de mejora de la seguridad del área de sistemas de la UGEL Sullana?, lo que generó que proponga el siguiente objetivo general aplicar metodologías de evaluación de riesgos informáticos para proponer un plan de mejora de la seguridad del área de sistemas de la UGEL Sullana.

Con este propósito, se utilizó el tipo de investigación cuantitativa, de nivel descriptivo y diseño no experimental de corte transversal. Dicha investigación tiene una justificación académica ya que permite aplicar los conocimientos adquiridos en nuestra formación, tecnológica pues hacemos frente a épocas en que es difícil encontrar una organización que no cuente con la tecnología de última generación en cuanto a redes y comunicaciones. Además, se presentan los resultados de la investigación junto a las conclusiones y recomendaciones.

Capítulo 1

Evaluación de riesgos informáticos.

Contexto: gestión de riesgos de tecnología

Molina (2015), en la tesis titulada "Propuesta de un plan de gestión de riesgos de tecnología aplicado en la Escuela Superior Politécnica del Litoral", sostiene que los riesgos están presentes en todo ámbito laboral y pueden provocar muchas pérdidas en el negocio si no son controladas a tiempo y de forma adecuada. Para ello existen procesos como es el caso de la gestión de los riesgos tecnológicos cuya finalidad es la protección de la información, conociendo las fortalezas y debilidades que pudiesen afectar durante todo el ciclo de vida del servicio. En el presente trabajo se han descrito los conceptos relacionados con la gestión de los riesgos de la seguridad de la información, estándares, metodologías y herramientas que proporcionan las guías necesarias para reducir el nivel de vulnerabilidad que tienen los activos ante una amenaza. Es de vital importancia que una organización, dedicada a brindar servicios tecnológicos y mantener respaldada mucha información confidencial de forma segura, cuente con un plan de gestión de riesgos para garantizar la continuidad del negocio. Por este motivo, se ha visto la necesidad de desarrollar un análisis de riesgo tecnológico de orden cualitativo aplicado en el centro que administra y brinda los servicios de red y sistemas de la Escuela Superior Politécnica del Litoral siguiendo la metodología MAGERIT. Primero se procede a describir la situación actual de la organización, luego a identificar los activos con sus respectivas amenazas, para proseguir a realizar la medición de riesgos existentes y sugerir las salvaguardas necesarias que podrían formar parte del plan de implantación. Para la evaluación se ha considerado la herramienta PILAR, la cual so-

porta el análisis y gestión de los riesgos de sistemas de información siguiendo la metodología MAGERIT. Los resultados muestran los gráficos que reflejan los niveles de riesgo e impacto potencial, actual y objetivo. Finalmente, la aportación de este estudio es identificar el nivel de riesgo en que se encuentran los activos mediante el nivel de madurez de la seguridad implementada y sobre todo incentivar al personal a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recursos.

En el año 2015, Álvarez & Guanoluisa realizaron el trabajo de investigación titulado: "Auditoría a los Procesos de Desarrollo de Software del Centro de Transferencia Tecnológica de la ESPE para el caso del Sistema Hospitalario HB11 bajo el Marco de Referencia COBIT 5", Este trabajo se enfoca en: 1) la definición de mecanismos e instrumentos a utilizar para la auditoría puesto que COBIT 5 sólo es una mejor práctica y no una metodología y 2) la auditoria, para el primer enfoque se considera que COBIT ofrece flexibilidad ya que se apega a las necesidades particulares de cada organización. Por ello se inicia con la selección de objetivos de Gobierno y TI tanto en el CTT como en el Hospital HB11 con la participación del personal designado, realizarlo en ambas entidades permite detectar el nivel de importancia o aporte estratégico que tiene el sistema de información en cada una. Luego se continúa con la selección de procesos facilitadores y prácticas de gobierno seleccionadas por los interesados y mapeados con los procesos de desarrollo CTT. Para la evaluación del nivel de capacidad se conjuga los elementos de escala y atributos de capacidad por cada proceso facilitador y práctica de gobierno y se inicia por valorar si el nivel uno ha sido cumplido puesto que cada nivel de capacidad

puede ser alcanzado sólo cuando el nivel inferior se ha cumplido por completo. Los resultados se presentan con gráficos radares y tablas que identifican las brechas entre porcentajes óptimos y porcentajes alcanzados por el CTT, mientras que la emisión de recomendaciones de auditoria se realiza por cada proceso facilitador y práctica de gobierno, estas recomendaciones se presentan a nivel de listado de actividades a realizar para lograr un resultado exitoso y minimizar la brecha existente.

Aguirre y Palacios (2014), realizaron el trabajo de investigación titulado: "Auditoría a los Procesos de Desarrollo de Software del Centro de Transferencia Tecnológica de la ESPE para el caso del Sistema Hospitalario HB11 bajo el Marco de Referencia COBIT 5". El MDMQ maneja información sensible de la ciudadanía, como lo es la información catastral, licencia metropolitana única para el ejercicio de actividades económicas, pagos de impuestos prediales, declaración de patente y 1,5 x 1000 en activos, regularización de edificaciones existentes entre otras. Dicha información es crítica la cual se encuentra alojada en los servidores y sistemas de almacenamiento ubicados en el Data Center, por lo que es necesario que se garantice su confidencialidad, integridad y disponibilidad. El presente trabajo se orienta a la evaluación técnica informática para determinar el cumplimiento de las normas y estándares internacionales que establecen un GAP de la gestión de seguridad de la información, según las normas ISO/IEC 27001:2005 SGSI e ISO/IEC 27002:2005. Cabe señalar que dicho trabajo, se desarrollará mediante una investigación documental – descriptiva, para la recolección de la información se empleará técnicas de investigación de campo de fuentes primarias, como son la observancia

y la entrevista; y secundarias como son documentos y libros dicha información, será analizada y evaluada, mediante lo cual, se determinará el cumplimiento o no de los lineamientos según la norma ISO/IEC 27002:2005, con el fin de identificar vulnerabilidades de seguridad en el de todos los elementos que se encuentran en Data Center y recomendar se establezcan políticas de seguridad de la información y se implemente controles para el manejo de riesgos, monitoreo y revisión de desempeño y efectividad del Data Center, considerando el mejoramiento continuo de la seguridad.

Sistema de gestión de seguridad en Perú

Barrantes y Hugo Herrera (2012), en su tesis titulada "Diseño e implementación de un sistema de gestión de seguridad de información en procesos tecnológicos", determinan que, en la actualidad, muchas empresas que están o desean incursionar en el ámbito financiero tienen problemas para resguardar la seguridad de su información; en consecuencia, esta corre riesgos al igual que sus activos. El propósito de este trabajo se centró en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), bajo una metodología de análisis y evaluación de riesgos desarrollada y diseñada por los autores de este trabajo, también se usaron como referencias las normas ISO 27001:2005 e ISO 17799:2005. Esta implementación permitió un gran aumento en la seguridad de los activos de información de la empresa Card Perú S.A., que garantiza que los riesgos de seguridad de información sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible, eficiente y

adaptable ante los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Alfaro (2008), en su trabajo titulado: "Metodología para la auditoría integral de la gestión de la tecnología de información", presenta la revisión de la literatura sobre estándares internacionales de calidad relacionados a la gestión de tecnología de información (COBIT, ISO/IEC 12207, ISO/IEC 17799, ISO/IEC 20000 (ITIL), PMBOK, ISO/IEC 27001, IEEE 1058-1998, ISO 9001:2000 e ISO 19011:2002), MoProSoft 1.3, y las normas relacionadas a la auditoría informática en el Estado Peruano, se concluye que no existe una metodología para la auditoría integral de la gestión de la tecnología de información. Los enfoques actuales están basados sobre el proceso general de auditoría sumándoles las inclusiones no integradas de los diversos estándares de calidad internacional, o las normas vigentes para las entidades que son sujetas de evaluación en una auditoría. El objetivo de la tesis fue el desarrollo de una metodología para la auditoría integral de la gestión de las tecnologías de información (MAIGTI), con un enfoque de procesos, basado en estándares de calidad internacionales.

Por otra parte, Villena (2006), en su tesis titulada "Sistema de gestión de seguridad de información para una institución financiera", sostiene que, en la actualidad, las inversiones en seguridad que realizan las empresas se destinan cada vez menos a la compra de productos, destinando más bien parte de su presupuesto a la gestión de la seguridad de la información. El concepto de seguridad ha variado, acuñándose uno nuevo, el de seguridad gestionada, que va desplazando poco a poco al de "seguridad informática".

Las medidas que comienzan a tomar las empresas giran en torno al nuevo concepto de gestión de la seguridad de la información. Éste tiene tres vertientes: técnica, legal y organizativa, es decir, un planteamiento coherente de directivas, procedimientos y criterios que permiten desde la administración de las empresas asegurar la evolución eficiente de la seguridad de los sistemas de información, la organización afín y sus infraestructuras. Para gestionar la seguridad de la información de una entidad se debe partir de una premisa fundamental y es que la seguridad absoluta no existe. Tomando lo anterior como punto de partida, una entidad puede adoptar algunas de las normas existentes en el mercado que establecen determinadas reglas o estándares que sirven de guía para gestionar la seguridad de la información, La presente tesis ha realizado una investigación de las normas y estándares que van difundiéndose con mayor énfasis en el mercado peruano, en especial en el sector financiero. Se rescataron los aspectos más saltantes de cada norma y estándar, a partir de los cuales se plantea un esquema de gestión de seguridad de información que puede ser empleado por una institución financiera en el Perú, lo cual permitirá que ésta cumpla con las normas de regulación vigentes en lo relacionado a la Seguridad de Información.

Evaluación de riesgos en Piura

Carbajal (2013), en "Definición de una metodología para la elaboración de auditorías de sistemas informáticos en entidades del Sistema Nacional de Control Peruano", se propuso el objetivo

principal de proponer una metodología que permita guiar a los auditores gubernamentales del Sistema Nacional de Control Peruano en las auditorías de sistemas informáticos que se realizan en el sector público peruano. La presente guía metodológica se ha realizado en concordancia al marco normativo aplicable a las entidades del Sistema Nacional de Control Peruano utilizando en su elaboración los marcos de referencia de organismos internacionales. Dicha guía metodológica se convierte en una herramienta de consulta para los auditores gubernamentales que realizan auditorías en el sector público, contribuyendo de esta manera a realizar auditorías de una manera más eficiente y eficaz, facilitando la identificación de riesgos asociados a los controles de los procesos informáticos auditados, así como optimizar el tiempo invertido en la realización de auditorías de tipo informático.

Marchand (2013), en su tesis titulada "Metodología de implantación del modelo balanced scorecard para la gestión estratégica de TIC. Caso: Universidad Nacional Agraria De La Selva" considera que el despliegue de la metodología propuesta para la implantación del modelo de Balanced Scorecard (BSC) para la gestión estratégica de Tecnologías de Información y Comunicación (TIC), consta de seis fases, siendo la información de entrada, el plan estratégico de la institución, e iniciar el proceso de implantación con, la determinación del nivel de madurez de gestión de TIC en la organización, análisis del soporte actual, determinación de los objetivos estratégicos de TIC, determinación de indicadores e inductores para la gestión estratégica de TIC, construcción del CMI, y la revisión de métricas. El objetivo es encontrar, en primer

lugar, la brecha que existe entre los esfuerzos de TIC y las estrategias de la organización expresadas en los procesos y dependencias; en segundo lugar, establecer las acciones que permitan cerrar esa brecha y hacer uso del modelo de BSC para la gestión, que deviene en el monitoreo, control y acciones correctivas y preventivas. La metodología pasa por un proceso de validación mediante reuniones y entrevistas con los funcionarios y usuarios cuyo resultado se refleja en la construcción del cuadro de mando integral orientada a las estrategias organizacionales.

El caso de la Unidad de gestión educativa local Sullana– UGEL Sullana

Reseña Histórica

La institución desde su creación en la ciudad de Sullana ha presentado la siguiente evolución (UGEL Sullana, s.f.). En el año 1982 durante el segundo gobierno del Arq. Fernando Belaunde Terry, se da inicio al proceso de descentralización administrativa en la educación, es así que el 26 de marzo del mismo año con Resolución Ministerial Nº 007-82 ED, se aprueba el funcionamiento de la zona Nº 94 de Sullana, que tenía a su cargo las provincias de: Sullana, Ayabaca, Talara y Paita. Con el paso del tiempo en 1994 el gobierno de aquel entonces decide darle autonomía a cada provincia dejando de lado la denominación de Zona de Educación para pasar a convertirse en Unidad de Servicios Educativos – USE, en donde cada provincia pasó a administrar sus propias jurisdicciones;

tres años más tarde se crea la subregión de educación "Luciano Castillo Colonna" conformada por la provincia de Paita, Talara, Sullana y Ayabaca.

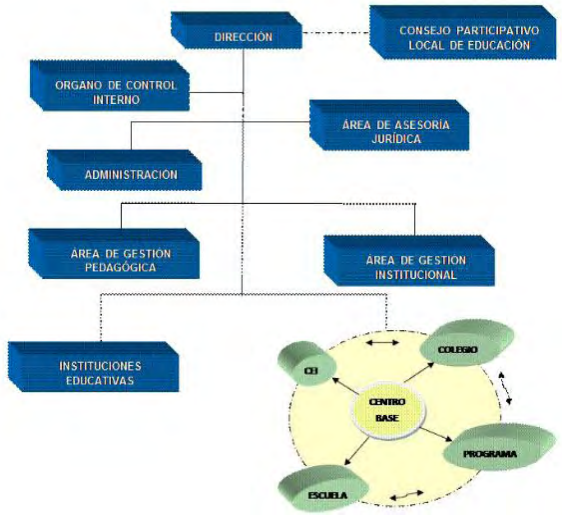
La Unidad de Gestión Educativa Local de Sullana creada el 05 de setiembre de 2003 Con Resolución Ejecutiva Regional Nº 0935-2003-GOB.REG.PIURA-PR, tiene a su cargo los distritos del ámbito de Sullana además por la cercanía administrativamente se incorpora Sapillica de la provincia de Ayabaca. Así mismo, cuenta en su ámbito jurisdiccional con 645 instituciones educativas públicas y privadas de los niveles de Inicial, Primaria, Secundaria, Básica Alternativa y Técnico Productiva.

El primer director de este ente descentralizado de educación fue el Dr. Guillermo Enrique Burneo Cardo, pasando luego más de diez ilustres profesores que han sabido conducir con acierto está sede institucional. Actualmente la Unidad de Gestión Educativa Local Sullana, mediante Resolución Directoral Regional N° 6177 – 2016 del 26 de julio del 2016, es dirigida por el Mg. Miguel Ángel Lizano Troncos, Director de UGEL Sullana, responsable de orientar conducir, supervisar, controlar y evaluar el servicio educativo en la jurisdicción.

Con el slogan "Trabajando en equipo por una educación de calidad", la actual gestión conduce y evalúa el servicio educativo en nuestra provincia.

Organización

Gráfico 1. Organigrama institucional



Fuente: Organigrama UGEL Sullana (s.f), More Reaño (2017)

Órgano de dirección

En el artículo 12 del Manual de Organización y Funciones (UGEL Sullana, s.f.), el director es el representante Legal de la Unidad de Gestión Educativa Local es el funcionario con el mayor nivel jerárquico en su ámbito, con autoridad y facultad para adoptar decisiones resolutivas y administrativas de acuerdo con la Ley.

Es un cargo de confianza del director regional de Educación de Piura, al que se accede por designación entre los postulantes mejor calificados en el correspondiente concurso. Su permanencia o remoción está sujeta a evaluación por parte de la Dirección Re-

gional de Educación con participación del Gobierno Regional, de acuerdo con norma específica expedida por el Ministerio de Educación.

Es el responsable de conducir la gestión institucional de la Unidad de Gestión Educativa Local de Sullana, en concordancia con las Normas emanadas del Ministerio de Educación y de la Dirección Regional de Educación de Piura y los lineamientos de Política Educativa Nacional y Regional.

Estructura orgánica interna

El Órgano de Dirección está constituido por:

- Director de Programa Sectorial III
- Relacionista Público I
- Especialista Administrativo I
- Técnico Administrativo I (2)
- Secretaria II
- Oficinista II

Órgano de control institucional

La Oficina de Control Institucional es el Órgano de Control de la Unidad de Gestión Educativa Local, responsable de realizar el control previo, simultaneo y posterior en las diferentes Unidades Orgánicas de la Unidad de Gestión Educativa Local y de las Instituciones y Programas Educativos de su ámbito jurisdiccional; cau-

telando la legalidad, eficiencia, eficacia y economía de sus actos y operaciones; así como el logro de sus objetivos para contribuir con el cumplimiento de los fines y metas institucionales. Tiene dependencia Administrativa y Funcional de la Contraloría General de la República y remunerativamente del Ministerio de Educación, las funciones del Órgano de Control están reguladas en la Ley 27785 Ley del Sistema Nacional de Control y de la Contraloría General de la República y la Resolución de Contraloría N° 459-2008-CG, Reglamento de los Órganos de Control Institucional, su sigla es OCI.

Estructura orgánica interna

El órgano de control está constituido por:

- Director de Sistema Administrativo II
- Especialista en Inspectoría I
- Secretaría I

Órgano de apoyo

Es el órgano responsable de conducir los sistemas administrativos de personal, abastecimiento, contabilidad, infraestructura, tesorería, es decir el desarrollo del potencial humano, contable, financiero, bienes y servicios de la Unidad de Gestión Educativa Local de Sullana y su jurisdicción en concordancia con las normas del Ministerio de Educación, de la Dirección Regional de Educación de Piura y los lineamientos de política educativa nacional y regional, en acción directa hacia las Instituciones Educativas.

Estructura orgánica interna

El Área de Gestión Administrativa, Infraestructura y Equipamiento está constituido por:

- Director de Sistema Administrativo II.
- Especialista Administrativo II.
- Especialista Administrativo I (02).
- Asistenta Social I.
- Tesorero I.
- Contador I.
- Ingeniero I.
- Cajero I.
- Técnico Administrativo I (05).
- Chofer I.
- Secretaria I.
- Oficinista II.

Área de gestión institucional

Es el órgano responsable de llevar a cabo la acción de asesoramiento, monitoreo y seguimiento de la labor institucional en los sistemas de planificación, Finanzas(presupuesto), estadística y racionalización de la Unidad de Gestión Educativa Local de Sullana y su jurisdicción en concordancia con las Normas emanadas por el Ministerio de Educación, Ministerio de Economía y Finanzas, Gobierno Regional y de la Dirección Regional de Educación de Piura y los lineamientos de política educativa nacional y regional, en acción directa hacia las Instituciones Educativas.

Estructura orgánica interna

El Área de Gestión Institucional tiene la siguiente organización interna:

- Director de Sistema Administrativo II
- Planificador I
- Estadística I
- Especialista en Racionalización I
- Especialista en Finanzas I
- Analista de Sistema PAD I
- Secretaría I

Información

Al respecto Lapiedra et al. (2011), sostienen que toda persona, toda empresa, y en general toda organización, está continuamente captando una serie de datos, gran parte de los cuales no tienen significación alguna para ella, pero en cambio existen otros datos que le sirven para conocer mejor el entorno que le rodea y también para conocerse mejor. Estos datos, que constituyen la llamada información, le van a permitir tomar decisiones más acertadas. Por ello, la información a tiempo y en la cantidad precisa es un factor clave para toda organización.

Seguridad de la información

Jiménez (2009), establece que los beneficios de un sistema de seguridad bien elaborado son inmediatos, ya que el la organización trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos: Aumento de la productividad. Aumento de la motivación del personal. Compromiso con la misión de la compañía. Mejora de las relaciones laborales. Ayuda a formar equipos competentes. Mejora de los climas laborales para los RR.HH.

Políticas de seguridad

Peso y Ramos (2015), consideran que para algunos las políticas han de incluir objetivos, creencias, niveles de ética y determinación de responsabilidades, pero consideramos que es un enfoque ambicioso si pensamos en que en muchas de las entidades no exis-

ten aún. En algunas entidades denominan políticas a las diferentes normas generales referidas a la seguridad de la información, y en otras reservan la denominación de política para la genérica, con una o dos páginas, y denominan normas a las del siguiente nivel. Las políticas, por su propia esencia, han de ser obligatorias, frente a guías o recomendaciones en las entidades, que pueden ser opcionales o explicativas.

Auditoría

Derrien (2009), acerca del objetivo de la auditoría sostiene que si exceptuamos el caso en el cual el término de auditoría informática designa, además de una manera impropia, la utilización del instrumento informático en el marco de una misión más amplia (auditoría contable, auditoría financiera, auditoría operacional), el objetivo principal de una auditoría informática es siempre el mismo: comprobar la fiabilidad de la herramienta informática y la utilización que se hace de la misma.

Análisis de riesgos de los sistemas de información

Para Chicano (2014), los sistemas de información de las organizaciones tienen multitud de recursos vulnerables ante ataques de seguridad. Por ello, es necesario que desarrollen estrategias y herramientas que sean capaces de identificar y valorar estos recursos y que, a su vez, puedan dar información sobre los ataques y daños que pueden afectarles. Las herramientas de gestión de riesgos sirven precisamente para estas funcionalidades: ayudan a identificar los recursos importantes en la organización, los riesgos a los que están sometidos y el daño que pueden sufrir en caso de producirse una amenaza de cualquier tipo.

De igual forma (2014), sostiene que un riesgo es un evento o conjunto de eventos que puede poner en peligro un proyecto de la organización o que puede impedir su éxito. La definición de riesgo en sí siempre ha ocasionado grandes debates. Aun así, existe un acuerdo sobre las características comunes que debe tener todo riesgo informático:

- Incertidumbre: el evento que caracteriza al riesgo puede ocurrir o no ocurrir, no hay certeza sobre su ocurrencia.
- Pérdida: en caso de materializarse el riesgo, habría varias consecuencias negativas para la organización. Si no hay efectos negativos, no hay riesgo en sí.
- Es bastante común la confusión entre las definiciones de problema, preocupación y riesgo, siendo necesario conocer sus diferencias (Chicano, 2014).
- Una preocupación es una situación sobre la que hay du-

das y que deberá ser evaluada como un posible riesgo. No obstante, analizada la preocupación es posible que se determine que no

- existen efectos negativos y que, por tanto, no se puede considerar riesgo.
- Un problema, sin embargo, es un riesgo que ya se ha materializado. En este caso, no hay incertidumbre, ya que hay certeza sobre su ocurrencia y, por tanto, tampoco se puede considerar riesgo.

En el gráfico se puede observar la diferencia entre los conceptos propuestos.

Gráfico 2. Problema, preocupación y riesgo

Fuente: Análisis de riesgos (Chicano, 2014; More Reaño, 2017).

Metodologías para análisis de riesgos informáticos

MAGERIT

El Consejo Superior de Administración Electrónica, dentro del Ministerio de Administraciones Públicas, publicó en 2006 una Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) según Giménez (2014). Como reconoce en su propia introducción, el gran reto de los métodos de análisis de riesgo, es la complejidad del problema al que se enfrentan, ya que hay muchos elementos que considerar, y si no se es riguroso, las conclusiones serán poco fiables. Se trata, por lo tanto, de encontrar una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista. Como también señala este método, el temor a lo desconocido es el principal origen de la desconfianza, de manera que un AGR busca conocer para confiar: conocer los riesgos para poder afrontarlos y controlarlos. El método pretende ser exhaustivo, en cuanto a recoger todo tipo de activos, todo tipo de activos de seguridad, y todo tipo de situaciones (Giménez, 2014).

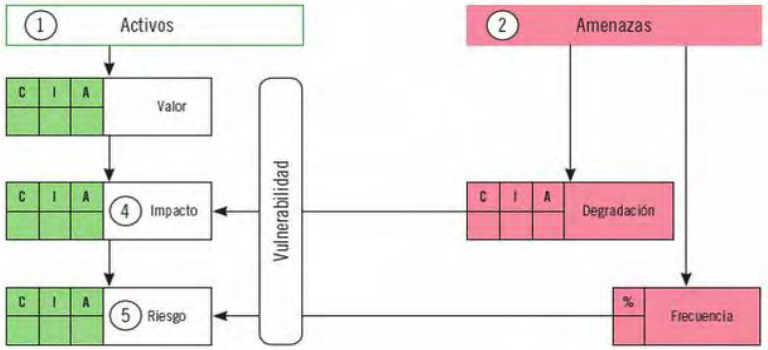
Análisis de riesgos

Según Giménez (2014), Se trata de ejecutar 5 pasos sencillos, para obtener una lista de los riesgos que soporta el sistema de información:

- Paso 1: determinar los activos y su valoración de C, I y A.

- Paso 2: determinar las amenazas, cuánto degradan la C, I y A de un activo, y con qué frecuencia o probabilidad aparecen.
- Paso 3: determinar las salvaguardas existentes y su eficacia (cuánto evitan la degradación C, I, y A de un activo, y cuánto reducen la frecuencia de la amenaza).
- Paso 4: determinar el impacto, o medida del daño posible al activo por la materialización de una amenaza.
- Paso 5: determinar el riesgo, o medida del daño probable al activo (impacto ponderado por la tasa de ocurrencia de la amenaza).

Gráfico 3. Elementos del Análisis de Riesgos

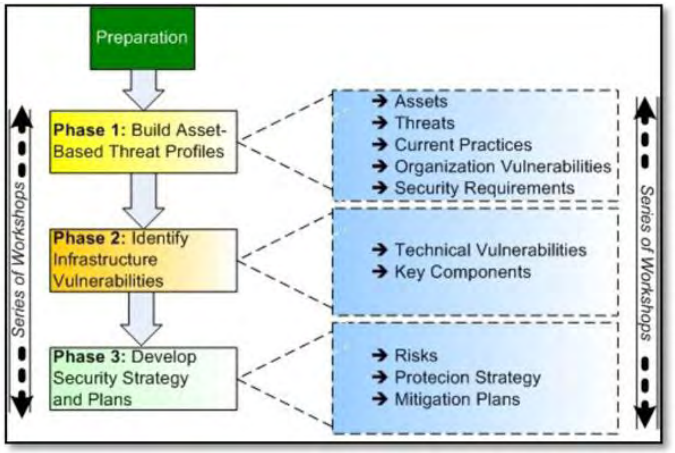


Fuente: Seguridad en equipos informáticos (Giménez, 2014; More Reaño, 2017).

OCTAVE

En el libro Seguridad en Equipos Informáticos, Gimenez (17), describe que son las siglas de Operationally Critical Threat, Asset and Vulnerability Evaluation. El método está desarrollado por la Universidad de Carnegie Mellon, y define un conjunto de criterios, para poder emplear métodos más flexibles según la empresa. Existen tres métodos muy comunes que cumplen esos criterios de compatibilidad: el método OCTAVE original, el OCTAVE-S para pequeñas empresas, y el OCTAVE- Allegro, especialmente centrado en los activos de información. Los criterios son bastante generales, e incluyen: que las medidas sean adaptables a las necesidades, que el proceso de análisis esté definido, sea continuo y tenga visión de futuro, y que el proceso se centre en un conjunto reducido de riesgos críticos. Los resultados se dividen en diferentes fases: una fase organizativa (activos críticos y sus requerimientos, amenazas, y prácticas de seguridad habituales), una fase tecnológica (componentes clave y vulnerabilidades), y una tercera y última fase estratégica, o de desarrollo del plan de riesgos.

Gráfico 4. Fases OCTAVE

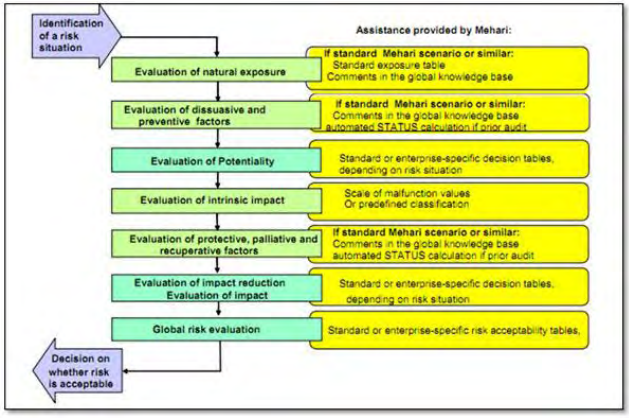


Fuente: Seguridad en el trabajo (Huerta, 2012; More Reaño, 2017).

MEHARI

Según Huerta (2012), MEHARI es la metodología de análisis y gestión de riesgos desarrollada por la CLUSIF (*Club de la Sécurité de l'Information Français*) en 1995 y deriva de las metodologías previas Melissa y Marion. La metodología ha evolucionado proporcionando una guía de implantación de la seguridad en una entidad a lo largo del ciclo de vida. Del mismo modo, evalúa riesgos en base a los criterios de disponibilidad, integridad y confidencialidad.

Gráfico. 5 Metodología MEHARI



Fuente: Proceso de análisis de riesgo (Huerta, 2012; More Reaño, 2017).

Comparación metodologías

MAGERIT	OCTAVE	MEHARI
Gutiérrez (2013). -Se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad. -Permite identificar claramente las medidas preventivas y correctivas más apropiadas. -Presenta una guía completa y paso a paso de cómo llevar a cabo el análisis de riesgos -Contiene una división de los activos de información que deben considerarse. -Cuenta con un listado de amenazas y controles que deben tenerse en cuenta. -Describe diferentes técnicas frecuentemente utilizadas en el análisis de riesgos. -Es útil para aquellas empresas que inicien con la gestión de la seguridad de la información. -Esta alineado con los estándares de ISO lo que permite que su implementación se convierte en el punto de partida para una certificación o para mejorar los sistemas de gestión. Gutiérrez (2013).	Enríquez (2013). -Se centra en el estudio de riesgos organizacionales, principalmente en los aspectos relacionados con el día a día de las empresas. -La evaluación inicia a partir de la identificación de los activos relacionados con la información. -Estudia la infraestructura de información y, más importante aún, la manera como dicha infraestructura se usa. -Contempla para su implementación la conformación de un equipo mixto, compuesto de personas de las áreas de negocios y de TI. - El proceso de evaluación contemplado por OCTAVE se divide en tres fases: Construcción de perfiles de amenazas basadas en activos, Identificación de vulnerabilidades en la infraestructura y desarrollo de estrategias y planes de seguridad.	Fontecha (2014). -Cuenta con una guía de análisis de riesgos, realizado mediante una evaluación cuantitativa y cualitativa. -Proporciona un método para la evaluación y gestión en el dominio de la seguridad de la información. -Permite un análisis directo e individual de situaciones de riesgos descritas en los escenarios. -Proporciona un conjunto de herramientas específicamente diseñadas para la gestión de la seguridad a corto, mediano y largo plazo, adaptables a diferentes niveles de madurez y tipos de acciones consideradas. -Se fundamenta en el principio de que las herramientas requeridas en cada fase del desarrollo de la seguridad deben ser consistentes. -Una situación de riesgo se puede caracterizar por diferentes factores: Factores estructurales y Factores de reducción del riesgo. -Permite la evaluación cualitativa y cuantitativa de los factores estructurales y de reducción del riesgo. - Integra cuestionarios de controles de seguridad, lo que permite evaluar el nivel de calidad de los mecanismos y soluciones encaminadas a la reducción del riesgo.

Fuente: More Reaño, 2017.

Aplicación De Magerit

Elementos básicos:

Activos

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos (Dirección General de Modernización Administrativa, 2012.

Activos esenciales: Información y servicios.

Activos relevantes: datos, servicios, equipos, aplicaciones informáticas, equipamiento auxiliar, etc.

Amenazas

Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. Las amenazas pueden ser de origen natural, del entorno, defectos de las aplicaciones, causadas de forma accidental o deliberada (Dirección General de Modernización Administrativa, 2012).

Salvaguardas

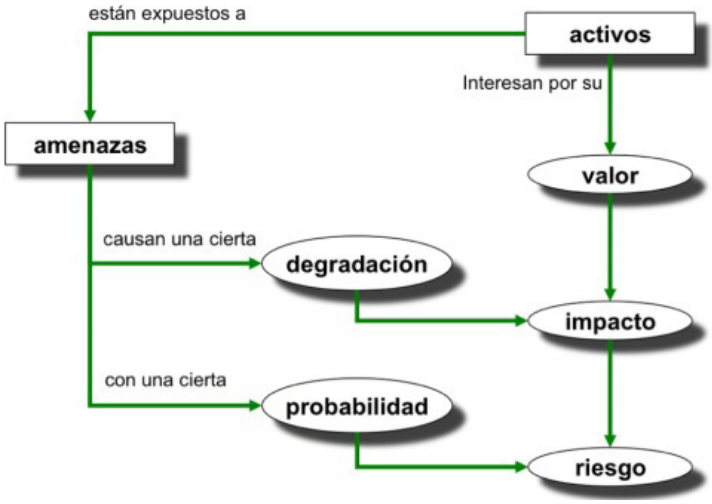
Aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo (Dirección General de Modernización Administrativa, 2012).

a) Método de análisis de riesgos

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados SEGÚN MAGERIT – versión 3.0 (Dirección General de Modernización Administrativa, 2012):

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación
2. Determinar a qué amenazas están expuestos aquellos activos.
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Gráfico 6. Elementos del análisis de riesgos potenciales



Fuente: Análisis de riesgos (Dirección General de Modernización Administrativa, 2012; More Reaño, 2017)

Formalización de las actividades

Este conjunto de actividades tiene los siguientes objetivos SEGÚN MAGERIT – versión 3.0 (Dirección General de Modernización Administrativa, 2012):

- Levantar un modelo del valor del sistema.
- Levantar un mapa de riesgos del sistema, identificando y valorando las amenazas sobre aquellos activos.
- Levantar salvaguardas.
- Evaluar el impacto posible sobre el sistema en estudio,

tanto el impacto potencial (sin salvaguardas), como el impacto residual (incluyendo el efecto de las salvaguardas desplegadas para proteger el sistema).

- Evaluar el riesgo del sistema en estudio, tanto el riesgo potencial (sin salvaguardas), como el riesgo residual.

b) Gestión de riesgos

Se destacan las siguientes actividades (Pita, S., y Pertégas, 2002):

- Evaluación de los niveles de impacto y riesgos residuales.
- Determinación de los niveles aceptables de riesgo.
- Estudios cualitativos y cuantitativos de costes/beneficios.
- Estrategias de tratamiento del riesgo: eliminación, mitigación, compartición y financiación.
- Documentación del proceso.

c) Plan de seguridad

Trata de cómo llevar a cabo planes de seguridad, para el tratamiento de los riesgos.

Estos planes reciben diferentes nombres en diferentes contextos y circunstancias:

- Plan de mejora de la seguridad
- Plan director de seguridad
- Plan estratégico de seguridad
- Plan de adecuación.

Se identifican 3 tareas:

- PS – Plan de Seguridad
- PS.1 – Identificación de proyectos de seguridad
- PS.2 – Plan de ejecución
- PS.3 – Ejecución

c) Desarrollo de sistemas de información

Según MAGERIT – versión 3.0 (Dirección General de Modernización Administrativa, 2012). Las aplicaciones constituyen un tipo de activos frecuente y nuclear para el tratamiento de la información en general y para la prestación de servicios basados en aquella información. La presencia de aplicaciones en un sistema de información es siempre una fuente de riesgo en el sentido de que constituyen un punto donde se pueden materializar amenazas.

El análisis de los riesgos constituye una pieza fundamental en el diseño y desarrollo de sistemas de información seguros. Es posible, e imperativo, incorporar durante la fase de desarrollo las funciones y mecanismos que refuerzan la seguridad del nuevo sistema y del propio proceso de desarrollo, asegurando su consistencia y seguridad, completando el plan de seguridad vigente en la Organización.

El Esquema Nacional de Seguridad recoge el riesgo como pieza fundamental de la seguridad de los sistemas en varios de sus principios básicos:

Hipótesis General: La aplicación de metodologías de evaluación de riesgos informáticos permitirá proponer un plan de mejora de la seguridad del área de sistemas de la UGEL Sullana – Piura.

Hipótesis Específicas

- La identificación y valoración de los activos relevantes del área de Sistemas de la UGEL Sullana permitirá elaborar el árbol de dependencias.
- La identificación y valoración de las amenazas que pueden afectar a los activos del área de Sistemas de la UGEL Sullana permitirá determinar el mapa de riesgos.
- La determinación de las salvaguardas permitirá identificar los principales riesgos informáticos del área de Sistemas de la UGEL Sullana.

Variable

El análisis del riesgo realizado a área de Sistemas de la UGEL Sullana permitirá elaborar el plan de mejora de la seguridad.

Metodologías de evaluación de riesgos informáticos.

Cómo identificar y valorar los activos relevantes del área de Sistemas de la UGEL Sullana

Tipo y Nivel de la Investigación

Tipo investigación, es cualitativo, según Pita y Pertégas (2002), investigación cualitativa evita la cuantificación. Los investigadores cualitativos hacen registros narrativos de los fenómenos que son estudiados mediante técnicas como la observación participante y las entrevistas.

Nivel de la investigación, es descriptivo, para Plasencia (2013), investigación es descriptiva porque su objetivo es llegar a conocer las situaciones, costumbres y actitudes predominantes a través de la descripción exacta de las actividades, objetos, procesos y personas, en esta investigación se examinan y describen las variables de estudio. Mientras que para Cazau (2006), las investigaciones descriptivas constituyen una mera descripción de algunos fenómenos, para lo que se centran en la medición de una o más variables dependientes en alguna población o muestra, Pero también indica que los estudios descriptivos sirven para analizar cómo es y se manifiesta un fenómeno y sus componentes (ejemplo, el nivel de aprovechamiento de un grupo, cuántas personas ven un programa televisivo y porqué lo ven o no, etc.), un ejemplo típico de estudio descriptivo es un censo nacional, porque en él se intenta describir varios aspectos en forma independiente: cantidad de habitantes, tipo de vivienda, nivel de ingresos, etc., sin pretender averiguar si hay o no alguna correlación, por ejemplo, entre nivel de ingresos y tipo de vivienda.

Diseño de la investigación

El diseño de investigación no experimental de acuerdo con Kerlinger (2002), es la búsqueda empírica y sistemática en la que el científico no posee control directo de las variables independientes, debido a que sus manifestaciones que han ocurrido o que son inherentemente no manipulables. Se hacen inferencias

sobre las relaciones entre las variables, sin intervención directa sobre la variación simultánea de las variables independiente y dependiente.

Además, la investigación de corte transversal, según Hernández (2016), que la define como la recopilación de datos en un solo momento, en un tiempo único. Su propósito es descubrir variables y analizar su incidencia e interrelación en un momento dado. Es como tomar una fotografía de algo que sucede.

El diseño de la investigación se gráfica de la siguiente manera:

Donde:

M —- > Muestra

O —- > Observación

Población y Muestra

Se ha delimitado la población en una cantidad de 12 trabajadores relacionados directamente al área de sistemas de la UGEL

de Sullana. Para efectos de la muestra esta ha sido seleccionada en base a la totalidad de la población, por lo cual contamos con una población muestral.

Definición y Operacionalización de las variables en estudio

Tabla 1. Matriz de Operacionalización de Variables

Variable	Definición conceptual	Dimensiones	Indicadores	Definición operacional
Metodologías de evaluación de riesgos informáticos	La evaluación de riesgos es el primer proceso en la metodología de gestión de riesgos. Las organizaciones utilizan la evaluación de riesgos para determinar el alcance de la amenaza potencial y el riesgo asociado Con un sistema de tecnología de la información a través del desarrollo del ciclo de vida del sistema. El resultado de este proceso ayuda a identificar los controles adecuados para reducir o eliminar los riesgos durante el proceso de mitigación de los mismos (28).	Análisis de la plataforma tecnológica actual. Análisis de procesos actuales. Análisis de riesgo en el área de sistemas. Evaluación de riesgos. Metodologías de evaluación de riesgos informáticos.	Número de herramientas TIC utilizadas. Existencia de procesos definidos. Debilidades y amenazas informáticas. Plan de contingencia. Enfoque de medición de riesgos y amenazas.	Si No

Fuente: More Reaño, 2017.

Técnicas e instrumentos

Observación directa

Según Namakforoosh (2005), la observación es la forma directa de recopilar datos en el momento que ocurren ciertos eventos, por lo que la observación directa se define como el método directo que describe la situación en la que el observador es físicamente presentado y personalmente maneja lo que sucede. Con esta técnica se pudo tener una percepción más clara del problema planteado, pudiendo observar la situación desde el enfoque de los usuarios como de los integrantes de la administración.

Encuesta

Según García (1992), una técnica de investigación realizada sobre una muestra de sujetos representativa de un colectivo más amplio, que se lleva a cabo en el contexto de la vida cotidiana, utilizando procedimientos estandarizados de interrogación. De igual forma se ha utilizado la entrevista.

Documentación

Recolección de documentación de la unidad de sistemas sobre los bienes informáticos y su estado; análisis de la red, etc.

Cuestionario

De acuerdo con Hernández (2016), define que el cuestionario es un género escrito que pretende acumular información por medio de una serie de preguntas sobre un tema determinado para, finalmente, dar puntuaciones globales sobre éste. De tal manera que, podemos afirmar que es un instrumento de investigación el que se utiliza para recabar, cuantificar, universalizar y finalmente, comparar la información recolectada. Como herramienta, el cuestionario es muy común en todas las áreas de estudio porque resulta ser una forma no costosa de investigación, que permite llegar a un mayor número de participantes. En la presente investigación se aplicó la matriz de valoración.

Validez del instrumento

El instrumento fue validado a través de la validación de contenido mediante el juicio de expertos. En tal sentido, se sometió al juicio de tres profesionales con grado de maestría, quienes revisaron y evaluaron la pertinencia, coherencia, congruencia, suficiencia, etc. Del instrumento, de acuerdo con la ficha de validación propuesta. Los resultados para el instrumento se indican en la tabla siguiente:

Instrumento	Experto 1	Experto 2	Experto 3	Promedio
O1	0,90	0,93	0,90	0,91

Tal como se observa, los tres profesionales han validado de manera favorable dicho instrumento, con un promedio de 0,91 lo cual corresponde a una validez muy buena, lo que significa que el instrumento está midiendo bien el concepto para el que ha sido preparado.

Plan de análisis

Luego de recogerse los datos, se empezó la tabulación de los resultados de cada pregunta en el programa Microsoft Excel versión 2013 y así se obtuvo los cuadros de tabulación donde se indica:

- Los ítems de preguntas
- Las alternativas de respuesta
- Las frecuencias absolutas
- Los porcentajes, se elaboran tablas y gráficos.

Matriz de consistencia

Tabla 2. Matriz de consistencia

Planeamiento del Problema	**Objetivo de la Investigación**	**Hipótesis de la Investigación**	**Variable de Estudio**	**Indicadores**	**Metodología de Investigación**
Enunciado del Problema ¿La aplicación de metodologías de evaluación de riesgos informáticos permite proponer un plan de mejora de la seguridad del área de sistemas de la UGEL Sullana?	Objetivo General Aplicar metodologías de evaluación de riesgos informáticos para proponer un plan de mejora de la seguridad del área de sistemas de la UGEL Sullana. Objetivos Específicos a) Identificar y valorar los activos relevantes del área de Sistemas de la UGEL Sullana. Identificar y valorar las amenazas que pueden afectar a los activos del área de Sistemas de la UGEL Sullana. Determinar las salvaguardas que permitan identificar los principales riesgos informáticos del área de Sistemas de la UGEL Sullana. Elaborar el plan de mejora de la seguridad del área de Sistemas de la UGEL Sullana.	Hipótesis General La aplicación de Metodologías de evaluación de riesgos informáticos permitirá proponer un plan de mejora de la seguridad del área de sistemas de la UGEL Sullana – Piura. Hipótesis Específicas a) La identificación y valoración de los activos relevantes del área de Sistemas de la UGEL Sullana permitirá elaborar el árbol de dependencias. b) La identificación y valoración de las amenazas que pueden afectar a los activos del área de Sistemas de la UGEL Sullana permitirá determinar el mapa de riesgos. c) La determinación de las salvaguardas permitirá identificar los principales riesgos informáticos del área de Sistemas de la UGEL Sullana. d) El análisis del riesgo realizado a área de Sistemas de la UGEL Sullana permitirá elaborar el plan de mejora de la seguridad.	Metodologías de Evaluación de riesgos informáticos	Activos existentes en la institución. Existencia de procesos definidos. Amenazas informáticas. Salvaguardas. Plan de contingencia.	El tipo y el nivel de la investigación Cualitativa Descriptiva Diseño de la investigación No Experimental y de acuerdo con la temporalidad de corte transversal.

Fuente: More Reaño (2017).

Capítulo 2

Proceso del análisis del riesgo

Identificación de activos por clases Equipos informáticos (Hardware) [HW]

HW001 — Servidores

HW002 — Computador personal

HW003 — Impresoras

HW004 — Conmutadores

Aplicaciones informáticas (Software) [SW]

SW01 — Sistema de Gestión de Base de Datos

SW02 — Sistemas de información

SW03 — Antivirus

SW04 — Sistema operativo

SW05 —Servidor de aplicaciones

SW06 — Servidor de correos

Datos/información [D]

D01–Archivos

D02 — Copias de Respaldo

D03 — Datos de control de acceso

D04 — Datos de configuración

Servicios [S]

S01 — Público en general

S02 — A usuarios externos

S03 — A usuarios internos

Instalaciones [L]

I01 — Centro Procesamiento de datos

I02 — Oficinas

Equipamiento auxiliar [AUX]

AUX01 — Equipo de climatización

AUX02 — Sistemas de alimentación ininterrumpida (UPS)

AUX 03 — Cableado Eléctrico/red

Personal [P]

P01 — Operadores

P02 — Administrador

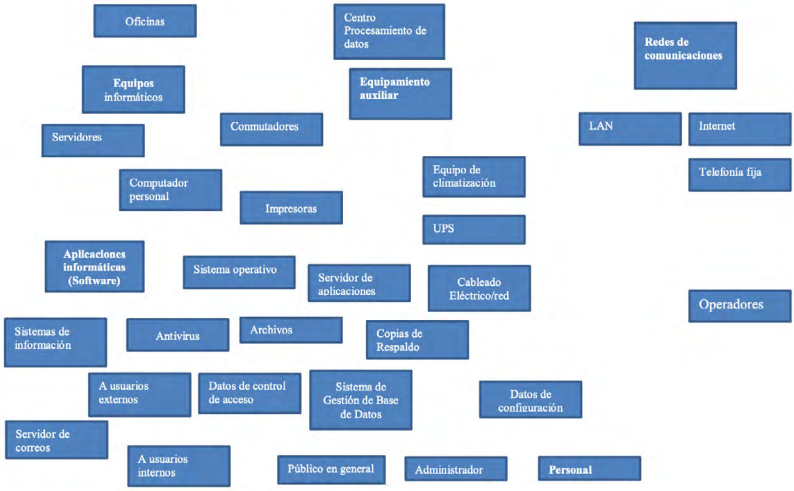
Redes de comunicaciones [COM]

COM01 — Internet

COM01 — LAN

COM03 — Telefonía fija

Árbol de dependencia de activos



Valoración de los activos

Tabla 3. Escala de criterios

	Valor	Criterio
10	Extremo	Daño extremadamente grave
9	Muy Alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Fuente: More Reaño (2017)

Las dimensiones de valoración:

D: Disponibilidad, poder utilizar el activo cuando se le requiere

I: Integridad de los datos, que el activo de información no se modifica de forma no autorizada.

C: Confidencialidad de la información, la información no se expone a personas no autorizadas.

Valoración de los equipos informáticos (hardware) identificados en la institución, según amenazas.

Tabla 4. Valoración de los equipos informáticos

Dimensión [HW]	**Servidores**			**Computador personal**			**Impresora s**			**Conmutadores**		
Amenaza	D	I	C	D	I	C	D	I	C	D	I	C
Fuego	10			10			10			10		
Daños por agua	10			9			9			10		
Corte de suministro eléctrico	2			2			2			2		
Terremoto	5			5			5			5		
Sobrecarga eléctrica	4			2			2			2		
Robo	10			10			10			10		
Falla de equipos de climatización	5											
Errores de configuración		7		4			2			5		
Desconexión físico o lógica	7			2			2			5		
Agotamiento de recursos	5						5					
Difusión de software dañino	7	7			7		2					
Errores de mantenimiento (Actualización de Harware)	7			5			2					
Errores de mantenimiento (Actualización de software)	7	9		5			2					
Acceso no autorizado		9	9			9						2
Errores de usuario					5		2					
Errores del administrador		7			5		2			3		

Fuente: More Reaño (2017)

Valoración de las aplicaciones informáticas (Software) identificados en la institución, según amenazas.

Tabla 5. Valoración de las aplicaciones informáticas (Software)

Dimensión [SW]	**Sistema de Gestión de Base de Datos**			**Sistemas de información**			**Antivirus**			**Sistema operativo**			**Servidor de aplicacion es**			**Servidor de correos**		
Amenaza	**D**	**I**	**C**	**D**	**I**	**C**	**D**	**I**	**C**	**D**	**I**	**C**	**D**	**I**	**C**	**D**	**I**	**C**
Fuego	4			4			4			4			4			4		
Corte de suministro eléctrico	5			5			5			5			4			4		
Terremoto	5			5			5			5			5			4		
Sobrecarga eléctrica	2			2			2			2			2			2		
Robo																		
Falla de equipos de climatización																		
Errores de configuración	5			5			4			5			5			5		
Desconexión físico o lógica	4			4			4			6			4			4		
Modificación deliberada de la información		9			9		2						9			9		
Difusión de software dañino	8	4		8	4		2			5			4			4		
Errores de mantenimiento (Actualización de hardware)	2			2			2			2			2			2		
Errores de mantenimiento (Actualización de software)	4			4			4			4			4			4		
Acceso no autorizado	5	5	5	5	5	5			3	5			5	5	5	5	5	5
Errores del administrador	6			6			2			6			6			6		

Fuente: More Reaño (2017)

Valoración de datos/información identificados en la institución, según amenazas.

Tabla 6. Valoración de datos/información

Dimensión [D]	**Archivos**			**Datos de control de acceso**			**Datos de configuración**		
Amenaza	D	I	C	D	I	C	D	I	C
Corte de suministro eléctrico	3			3			3		
Terremoto	5			5			5		
Sobrecarga eléctrica	2			2			2		
Robo	10			5			5		
Falla de equipos de climatización									
Errores de configuración	4			4			4		
Desconexión fisico o lógica	3			3			3		
Agotamiento de recursos									
Modificación deliberada de la información		8			8			5	
Difusión de software dañino	8			8			8		
Errores de mantenimiento (Actualización de Hardware)	2			2			2		
Errores de mantenimiento (Actualización de software)	5			5			5		
Acceso no autorizado			6			6			6
Errores de usuario									
Errores del administrador	5				5			5	

Fuente: More Reaño (2017)

Valoración de los servicios identificados en la institución, según amenazas.

Tabla 7. Valoración de los servicios

Dimensión [S]	**Público en general**			**A usuarios externos**			**A usuarios internos**		
Amenaza	D	I	C	D	I	C	D	I	C
Fuego	10								
Daños por agua	5			5			5		
Corte de suministro eléctrico	5			5			5		
Terremoto	8			8			8		
Sobrecarga eléctrica									
Robo									
Falla de equipos de climatización									
Errores de configuración									
Desconexión físico o lógica									
Agotamiento de recursos	3			3			3		
Modificación deliberada de la información									
Difusión de software dañino									
Errores de mantenimiento (Actualización de hardware)	3			3			3		
Errores de mantenimiento (Actualización de software)	3			3			3		
Acceso no autorizado									
Errores de usuario									
Errores del administrador	2			2			2		

Fuente: More Reaño (2017)

Valoración a las instalaciones identificadas en la institución, según amenazas.

Tabla 8. Valoración a las instalaciones

Dimensión [L]	Centro Procesamiento de datos			Oficinas		
Amenaza	D	I	C	D	I	C
Fuego	10			10		
Daños por agua	5			5		
Corte de suministro eléctrico	4			3		
Terremoto	10			10		
Sobrecarga eléctrica	2					
Robo	10			6		
Falla de equipos de climatización	5					
Errores de configuración						
Desconexión físico o lógica	8					
Agotamiento de recursos						
Modificación deliberada de la información						
Difusión de software dañino						
Errores de mantenimiento (Actualización de Hardware)						
Errores de mantenimiento (Actualización de software)						
Acceso no autorizado			5			
Errores de usuario						
Errores del administrador						

Fuente: More Reaño (2017)

Valoración del equipamiento auxiliar identificados en la institución, según amenazas.

Tabla 9. Valoración del equipamiento auxiliar

Dimensión [AUX]	Equipo de climatización			Sistemas de alimentación ininterrumpi da (UPS)			Cableado Eléctrico/red		
Amenaza	D	I	C	D	I	C	D	I	C
Fuego	10			10			10		
Daños por agua	6			6			2		
Corte de suministro eléctrico	6			6			5		
Terremoto	8			8			8		
Sobrecarga eléctrica	8			8			5		
Robo	10			10			10		
Falla de equipos de climatización	5			5					
Errores de configuración									
Desconexión físico o lógica	5			5			5		
Agotamiento de recursos									
Modificación deliberada de la información									
Difusión de software dañino									
Errores de mantenimiento (Actualización de hardware)									
Errores de mantenimiento (Actualización de software)									
Acceso no autorizado									
Errores de usuario									
Errores del administrador									

Fuente: More Reaño (2017)

Valoración que asigna al personal identificados en su institución, según amenazas.

Tabla N° 10: Valoración que asigna al personal

Dimensión [P]	Operador es			Administr ador		
Amenaza	D	I	C	D	I	C
Fuego	10			10		
Daños por agua	2			2		
Corte de suministro eléctrico						
Terremoto	8			8		
Sobrecarga eléctrica						
Robo						
Falla de equipos de climatización						
Errores de configuración						
Desconexión físico o lógica						
Agotamiento de recursos						
Modificación deliberada de la información						
Difusión de software dañino						
Errores de mantenimiento (Actualización de sofware)						
Errores de mantenimiento (Actualización de sofware)						
Acceso no autorizado			6			6
Errores de usuario						
Errores del administrador						

Fuente: More Reaño (2017)

Valoración que asigna a las redes de comunicaciones identificadas en su institución, según amenazas.

Tabla 11. Valoración que asigna a las redes de comunicaciones

Dimensión [AUX]	**Internet**			**LAN**			**Telefonía fija**		
Amenaza	D	I	C	D	I	C	D	I	C
Fuego	10			10			10		
Daños por agua	4			4			4		
Corte de suministro eléctrico	6			6			4		
Terremoto	8			8			5		
Sobrecarga eléctrica	5			5			2		
Robo									
Falla de equipos de climatización									
Errores de configuración	6			6					
Desconexión físico o lógica	5			5			5		
Agotamiento de recursos									
Modificación deliberada de la información									
Difusión de software dañino	5			5					
Errores de mantenimiento (Actualización de hardware)									
Errores de mantenimiento (Actualización de software)	5			5					
Acceso no autorizado			5			5			
Errores de usuario									
Errores del administrador	5			5			5		

Fuente: More Reaño (2017)

Valoración de amenazas por activos

Tabla 12. Escalas

ESCALAS		
Degradación	**Frecuencia**	**Riesgo**
MA: muy alto	MA: prácticamente seguro	MA: crítico
A: alto	A: probable	A: importante
M: medio	M: posible	M: apreciable
B: bajo	B: poco probable	B: bajo
MB: muy bajo	MB: muy raro	MB: despreciable

Fuente: More Reaño (2017)

Se escribe las abreviaturas que corresponden, según la escala cualitativa propuesta.

Tabla 13. Valoración de amenazas por activos

Tipos de Activos	Activos	Amenazas Relevantes	Degradación	Frecuencia	Riesgo
Equipos informáticos (Hardware)	Servidores	Fuego	MA	MB	M
		Terremoto	MA	MB	M
		Robo	A	MB	M
		Acceso no autorizado	A	M	A
		Falla de climatización	A	M	A
		Difusión de software dañino	A	M	A
	Computador de Personal	Fuego	MA	MB	M
		Terremoto	MA	MB	M
		Robo	A	M	A
		Acceso no autorizado	A	M	A
		Desconexión Física o lógica	B	M	M
		Difusión de software dañino	A	A	A
	Conmutadores	Fuego	MA	MB	M
		Terremoto	MA	MB	M
		Robo	MA	MB	M
		Desconexión físico o lógica	A	M	A

Tipos de Activos	Activos	Amenazas Relevantes	Degradación	Frecuencia	Riesgo
Aplicaciones informáticas (Software)	Sistema de Información	Errores de configuración	M	M	M
		Modificación deliberada de la información	A	M	A
		Acceso o autorizado	A	M	A
		Errores de usuario	B	M	M
	Sistema operativo	Errores de configuración	A	M	A
		Modificación deliberada de la información	A	M	A
		Acceso no autorizado	A	M	A
		Errores de usuario	B	MB	B
	Sistema de Gestión de Base de Datos	Errores de configuración	MA	M	A
		Modificación deliberada de la información	A	M	A
		Acceso no autorizado	A	M	A
		Errores de usuario	B	M	B
Datos/información	Archivos	Modificación deliberada de la información	A	M	A
		Acceso no autorizado	A	M	A
	Datos de control de acceso	Modificación deliberada de la información	A	M	A
		Acceso no autorizado	A	M	A
	Datos de configuración	Modificación deliberada de la información	A	M	A
		Acceso no autorizado	A	M	A
Servicios	Usuarios internos	Suplantación de la identidad del usuario	A		A
		Indisponibilidad de personal	B	B	B
		Errores del administrador	B	B	B
	Usuarios externos	Suplantación de la identidad del usuario	A	M	A
		Indisponibilidad de personal	A	M	A
		Errores de usuario	A	M	A

Tipos de Activos	Activos	Amenazas Relevantes	Degradación	Frecuencia	Riesgo
Instalaciones	Centro de datos	Incendio	MA	MB	M
		Terremoto	MA	MB	M
		Acceso no autorizado	A	M	A
		Daños por agua	A	MB	M
		Falla de equiposde climatización	A	M	A
Personal	Operadores	Suplantación de la identidad	A	M	A
		Corte de suministro eléctrico	M	M	M
		Errores del administrador	M	M	M
	Administradores	Errores de mantenimient o (Actualización de hardware)	A	M	A
		Acceso no autorizado	A	M	A

Tipos de Activos	Activos	Amenazas Relevantes	Degradación	Frecuencia	Riesgo
Equipamiento auxiliar	Equipo de climatización	Fuego	A	MB	M
		Daños por agua	A	MB	M
		Corte de suministro eléctrico	M	M	M
		Terremoto	A	MB	M
		Sobrecarga eléctrica	M	M	M
		Robo	MA	MB	M
	Sistemas de alimentación ininterrumpid a (UPS)	Fuego	MA	MB	M
		Daños por agua	A	MB	B
		Corte de suministro eléctrico	M	M	M
		Terremoto	MA	MB	M
		Sobrecarga eléctrica	B	B	B
		Robo	MA	M	A
	Cableado Eléctrico/ red	Fuego	MA	MB	M
		Daños por agua	A	MB	M
		Terremoto	A	MB	M
		Desconexión físico o lógica	M	M	M
		Robo	A	M	A
Redes de comunicaciones	Internet	Fuego	A	MB	M
		Daños por agua	M	MB	B
		Terremoto	A	MB	M
		Desconexión físico o lógica	A	MB	M
	LAN	Fuego	A	MB	M
		Daños por agua	A	MB	M
		Terremoto	A	MB	M
		Desconexión físico o lógica	M	MB	B
		Errores de configuración	A	B	M
		Acceso no autorizado	M	M	M

Fuente: More Reaño (2017)

Valoración de salvaguardas

Tabla 14. Eficacia y madurez de las salvaguardas

Factor	Nivel	Significado
0%	L0	Inexistente
20%	L1	Inicial/ad hoc
40%	L2	Reproducible pero intuitivo
60%	L3	Proceso definido
80%	L4	Gestionado y medible
100%	L5	Optimizado

Fuente: More Reaño (2017)

Tabla 15. Valoración de salvaguardas

Riesgo	Salvaguarda	Actual	Objetivo
Fuego	Instalación de sistemas contra incendio	L0	L3
	Uso y mantenimiento de extintores	L1	L3
	Desarrollo de plan de emergencia ante incendios	L0	L4
	Inspecciones de seguridad	L1	L2
Daño por agua	Desarrollo del plan de prevención física.	L0	L3
Corte de suministro eléctrico	Implementación de UPS	L2	L4
	Adquisición de generador eléctrico.	L0	L4
Terremoto	Plan de contingencia ante desastres	L2	L4
	Planificación de simulacros de sismos	L2	L4
Robo	Establecimiento de la seguridad las 24 horas.	L1	L3
	Afiliación seguros contra robo	L0	L3
	Instalación de cámaras vídeo.	L0	L3

Riesgo	Salvaguarda	Actual	Objetivo
Falla de equipos de climatización	Ejecución plan de mantenimiento preventivo periódico.	L0	L4
	Adquisición de equipo de climatización.	L0	L3
Errores de configuración	Establecer el plan de pruebas.	L0	L3
	Documentar acciones de configuración de software.	L0	L3
Desconexión físico o lógica	Plan de contingencia para funcionamiento y recuperación de servicios.	L0	L4
Modificación deliberada de la información	Plan de contingencia para funcionamiento y recuperación de servicios.	L0	L4
	Regular acceso a equipos informáticos.	L2	L4
	Establecimiento de plan de copias de respaldo de forma periódica.	L0	L4
Difusión de software dañino	Actualización de software antivirus malware.	L3	L5
	Establecimiento de procedimientos de acceso a archivos, direcciones web, etc.	L1	L3
	Realizar exploraciones de diagnóstico de forma periódica.	L0	L3
Errores de mantenimiento (Actualización de software)	Establecer el plan de pruebas.	L0	L3
	Documentar acciones de configuración de software	L0	L3
Acceso no autorizado	Regular acceso a equipos informáticos e instalaciones.	L1	L3
	Establecer grupo de seguridad de la información.	L0	L3
Errores de usuario	Implementación de manuales de procedimientos.	L1	L3
Errores del administrador	Establecer el plan de pruebas.	L0	L3
	Documentar acciones de configuración de software	L1	L3
	Implementación de manuales de procedimientos.	L0	L3

Fuente: More Reaño (2017)

Proceso de estado del riesgo

Se tiene en cuenta los datos de frecuencia:

Tabla 16. Escalas Proceso de estado del riesgo

ESCALAS		
Degradación	Frecuencia	Riesgo
MA: muy alto	MA: prácticamente seguro	MA: crítico
A: alto	A: probable	A: importante
M: medio	M: posible	M: apreciable
B: bajo	B: poco probable	B: bajo
MB: muy bajo	MB: muy raro	MB: despreciable

Fuente: More Reaño (2017)

Tabla 17. Valoración impacto y riesgo

Tipos de Activos	Activos	Amenazas Relevantes	Impacto potencial	Impacto actual	Impacto Objetivo	Riesgo potencial	Riesgo actual	Riesgo objetivo
Equipos informáticos (Hardware)	Servidores	Fuego	MA	A	M	MA	M	B
		Terremoto	MA	A	B	A	M	B
		Robo	A	M	B	A	M	B
		Acceso no autorizado	A	M	MB	A	M	B
		Falla de climatización	A	M	MB	M	B	MB
		Difusión de software dañino	A	M	B	A	M	B
	Computador de Personal	Fuego	MA	A	M	MA	M	B
		Terremoto	MA	A	B	A	M	B
		Robo	A	M	B	A	M	B
		Acceso no autorizado	A	M	B	A	M	B
		Desconexión Física o lógica	M	B	MB	M	B	MB
		Difusión de software dañino	A	M	B	A	M	B
	Conmutadores	Fuego	MA	A	M	MA	M	B
		Terremoto	MA	A	M	A	M	B
		Robo	MA	A	M	A	M	B
		Desconexión físico o lógica	A	M	B	A	M	B

Tipos de Activos	Activos	Amenazas Relevantes	Impacto potencial	Impacto actual	Impacto Objetivo	Riesgo potencial	Riesgo actual	Riesgo objetivo
Aplicaciones informáticas (Software)	Sistema de Información	Errores de configuración	A	M	B	A	M	B
		Modificación deliberada de la información	A	M	B	MA	A	M
		Acceso o autorizado	A	M	B	A	M	B
		Errores de usuario	A	M	B	A	M	B
	Sistema operativo	Errores de configuración	A	M	B	A	M	B
		Modificación deliberada de la información	A	M	B	MA	A	M
		Acceso no autorizado	A	M	B	A	M	B
		Errores de usuario	A	M	B	A	M	B
	Sistema de Gestión de Base de Datos	Errores de configuración	MA	A	M	A	M	B
		Modificación deliberada de la información	A	M	B	A	M	B
		Acceso no autorizado	A	M	B	A	M	B
		Errores de usuario	A	M	B	A	M	B
Datos/información	Archivos	Modificación deliberada de la información	MA	A	B	MA	A	M
		Acceso no autorizado	A	M	B	A	M	B
	Datos de control de acceso	Modificación deliberada de la información	MA	A	M	MA	A	M
		Acceso no autorizado	A	M	B	A	M	B
	Datos de configuración	Modificación deliberada de la información	A	M	B	MA	A	M
		Acceso no autorizado	A	M	B	A	M	B

Tipos de Activos	Activos	Amenazas Relevantes	Impacto potencial	Impacto actual	Impacto Objetivo	Riesgo potencial	Riesgo actual	Riesgo objetivo
Servicios	Usuarios internos	Suplantación de la identidad del usuario	A	M	B	A	M	B
		Indisponibilidad de personal	B	B	MB	B	B	MB
		Errores del administrador	A	M	B	A	M	B
	Usuarios externos	Suplantación de la identidad del usuario	A	M	M	A	M	B
		Indisponibilidad de personal	M	B	MB	M	B	MB
		Errores de usuario	A	M	B	A	M	B
Instalaciones	Centro de datos	Incendio	MA	A	M	A	M	B
		Terremoto	MA	A	M	A	M	B
		Acceso no autorizado	A	M	B	A	M	B
		Daños por agua	A	M	B	A	M	B
		Falla de equiposde climatización	A	M	B	A	M	B
Personal	Operadores	Suplantación de la identidad	A	M	M	A	M	B
		Corte de suministro eléctrico	M	B	MB	M	B	MB
		Errores del administrador	A	M	B	A	M	B
	Administradores	Errores de mantenimient o (Actualización de hardware)	A	M	B	A	M	B
		Acceso no autorizado	A	M	B	A	M	B

Tipos de Activos	Activos	Amenazas Relevantes	Impacto potencial	Impacto actual	Impacto Objetivo	Riesgo potencial	Riesgo actual	Riesgo objetivo
Equipamiento auxiliar	Equipo de climatización	Fuego	MA	A	M	A	M	B
		Daños por agua	A	M	B	A	M	B
		Corte de suministro eléctrico	M	B	MB	M	B	MB
		Terremoto	MA	A	M	A	M	B
		Sobrecarga eléctrica	M	B	MB	M	B	MB
		Robo	MA	A	M	A	M	B
	Sistemas de alimentación ininterrumpid a (UPS)	Fuego	MA	A	M	A	M	B
		Daños por agua	A	M	B	A	M	B
		Corte de suministro eléctrico	M	B	MB	M	B	MB
		Terremoto	MA	A	M	A	M	B
		Sobrecarga eléctrica	M	B	MB	M	B	MB
		Robo	MA	A	M	A	M	B
	Cableado Eléctrico/ red	Fuego	MA	A	M	A	M	B
		Daños por agua	A	M	B	A	M	B
		Terremoto	MA	A	M	A	M	B
		Desconexión físico o lógica	M	B	MB	M	B	MB
		Robo	MA	A	M	A	M	B

Tipos de Activos	Activos	Amenazas Relevantes	Impacto potencial	Impacto actual	Impacto Objetivo	Riesgo potencial	Riesgo actual	Riesgo objetivo
Redes de comunicaciones	Internet	Fuego	MA	A	M	A	M	B
		Daños por agua	A	M	B	A	M	B
		Terremoto	MA	A	M	A	M	B
		Desconexión físico o lógica	M	B	MB	M	B	MB
	LAN	Fuego	MA	A	M	A	M	B
		Daños por agua	A	M	B	A	M	B
		Terremoto	MA	A	M	A	M	B
		Desconexión físico o lógica	M	B	MB	M	B	MB
		Errores de configuración	MA	A	M	A	M	B
		Acceso no autorizado	M					

Fuente: More Reaño (2017)

Capítulo 3

Plan de Seguridad

A continuación, como producto del análisis de riesgos realizado en el área de Sistemas de la UGEL de Sullana se presenta las siguientes propuestas, las cuales tienen como propósito convertirse en una alternativa que de aplicarse mejorarían la organización de la institución respecto a riesgos a la que está expuesta.

Propuesta 1

Descripción

La UGEL de Sullana, institución a cargo del magisterio de la provincia. Actualmente dirige sus actividades encaminadas a brindar servicios a todo docente de su jurisdicción, trabajadores de la misma institución y al público en general. Habitualmente se produce el ingreso de personas a esta dependencia del estado y en la mayor parte de oficinas no se restringe el acceso; de igual forma ocurre el desplazamiento de los propios trabajadores entre oficinas, sin ningún procedimiento o norma de acceso a estas, lo que ha ocasionado en varias oportunidades pérdida de documentos, alteración de información, caos en el desplazamiento. Entre la problemática descrita se puede destacar una serie de situaciones que se constituyen en una amenaza, las mismas que pueden afectar seriamente no solamente a una determinada área u oficina sino a toda la organización, originadas por personal mal intencionado, por desconocimiento. Adicional se tiene que considerar los daños ocasionados por la propia naturaleza por lo cual se requiere de adoptar políticas que mejoren la seguridad de la Institución.

Objetivos

- Establecer cómo se organiza la institución y las funciones que le corresponden a cada trabajador.
- Crear el manual de organización y funciones para el responsable del área de sistemas de la institución.
- Restringir el acceso del personal a áreas donde labora.
- Asignar los equipos informáticos con cargo, usuario, contraseña y bajo responsabilidad de uso y deterioro.

Establecer política de monitoreo del acceso a los activos de datos/información.

Activo afectado:

- Archivos
- Datos de control de acceso
- Datos de configuración

Amenaza relevante:

- Modificación deliberada de la información
- Acceso no autorizado

Salvaguarda:

- Regular acceso a equipos informáticos e instalaciones.
- Establecer grupo de seguridad de la información.
- Plan de contingencia para funcionamiento y recuperación de servicios.
- Regular acceso a equipos informáticos.
- Establecimiento de plan de copias de respaldo de forma periódica.

Análisis de Resultados

La presente investigación tuvo como objetivo general: Aplicar metodologías de evaluación de riesgos informáticos para proponer un plan de mejora de la seguridad del área de sistemas de la UGEL Sullana.; se ha realizado la aplicación del instrumento que permitió conocer los activos, amenazas, salvaguardas e identificar los riesgos a los que está expuesta el área de Sistemas de la UGEL Sullana. En consecuencia, luego de analizados las valoraciones se realizó el siguiente análisis:

En relación con la identificación de los activos se realizó su valoración, de igual forma las amenazas a las que están expuestos los activos fueron valoradas, lo que permitió determinar las principales salvaguardas según MAGERIT. Se ha identificado los principales riesgos a los que está expuesta la organización en general. En lo que se refiere a equipos informáticos, software, datos/información, instalaciones, personal, equipamiento auxiliar se puede apreciar que se encuentra en un nivel de riesgo medio lo que amerita medidas de solución inmediata, lo que es similar a la investigación realizado por Carbajal (2013), en el año 2013 el cual propone una metodología para la elaboración de auditorías de sistemas informáticos en entidades del Sistema Nacional de Control Peruano, el presente trabajo de tesis tiene como objetivo principal proponer una metodología que permita guiar a los auditores gubernamentales del Sistema Nacional de Control Peruano en las auditorías de sistemas informáticos que se realizan en el sector público peruano.

Conclusiones

De acuerdo a los resultados obtenidos y analizados, se deduce que el nivel de riesgo al que está expuesto el área de sistemas y en general de la UGEL Sullana, requiere de mucha atención ya que sus activos relevantes están expuestos a varias amenazas que ocasionarían un notable impacto en ellos y afectarían el normal funcionamiento de esta que es brindar servicios a los docentes de las instituciones educativas de la provincia de Sullana, a sus mismos trabajadores como también al público en general. Por tanto, se requiere de tomar medidas que permitan eliminar o controlar el nivel de riesgo y esto se logrará con la propuesta de un plan de mejora de la seguridad que plantea alternativas de solución según la metodología elegida. Lo que permite concluir que la hipótesis general queda aceptada.

La aplicación de la metodología MAGERIT permitió identificar y valorar los activos relevantes los mismos que permitieron determinar la relación entre ellos y plantear el árbol de dependencias de activos, lo que concuerda con lo propuesto en la hipótesis; por lo tanto, esta queda aceptada.

La aplicación de la metodología MAGERIT permitió identificar y valorar las amenazas relevantes que pueden afectar a los activos de la institución, lo que permitió determinar el mapa de riesgos, lo que concuerda con lo propuesto en la hipótesis; por lo tanto, queda aceptada.

La aplicación de la metodología MAGERIT permitió determinar las principales salvaguardas y su nivel de madurez tanto en

la actualidad como el que se desearía que existiera, se logró identificar el nivel de riesgo al que está expuesto el área de sistemas y la institución en general, lo que concuerda con lo propuesto en la hipótesis; por lo tanto, queda aceptada.

El análisis del riesgo realizado con la Metodología MAGERIT ha permitido conocer la real situación del área de Sistemas de la UGEL de Sullana, y a la vez proporciona los elementos para plantear un plan de seguridad cuyo éxito de aplicación dependerá del compromiso que asuman cada uno de los agentes que la conforman, lo que concuerda con lo propuesto en la hipótesis; por lo tanto, queda aceptada.

Recomendaciones

Es conveniente que el personal directivo y los responsables del área de sistemas de la UGEL de Sullana reciban orientaciones y capacitaciones respecto a metodologías de evaluación de riesgos, así como de los principales estándares internacionales que le permitan reconocer las amenazas a las que están expuestos.

Se debe llevar un control adecuado de los activos de la institución, ya que de ellos depende su normal funcionamiento y que esta pueda brindar el servicio adecuado a sus trabajadores, docentes y al público e general.

Los equipos y otros medios de tratamiento de la información correspondientes a las diferentes áreas deben contar con los ambientes adecuados y destinados estrictamente para su fin, esto evitará los accesos indebidos de parte del personal trabajador de la UGEL así como de los usuarios.

Se debe tener en cuenta otros activos que si bien no existían en la institución representan un valioso aporte en la continuidad de las operaciones que se realizan a diario.

Referencias

Aguirre, D., y Palacios, J. (2014). *Evaluación técnica de seguridades del data center del Municipio de Quito según las NORMAS ISO/IEC 27001:2005 SGSIE ISO/IEC 27002:2005.* [Tesis de maestría, Universidad de las Fuerzas Armadas ESPE]. http://repositorio.espe.edu.ec/handle/21000/8303

Alfaro, E. (2008). *Metodología para la auditoría integral de la gestión de la tecnología de información.* [Tesis grado, Pontificia Universidad Católica del Perú]. http://hdl.handle.net/20.500.12404/1048

Álvarez, R., & Guanoluisa, G. (2015). *Auditoría a los Procesos de Desarrollo de Software del Centro de Transferencia Tecnológica de la ESPE para el caso del Sistema Hospitalario HB11 bajo el Marco de Referencia COBIT 5.* [Tesis de maestría, Universidad de las Fuerzas Armadas ESPE]. http://repositorio.espe.edu.ec/handle/21000/10302

Barrantes, C., y Hugo, J. (2012). *Diseño e implementación de un Sistema de Gestión de Seguridad de Información en procesos tecnológicos.* [Tesis pregrado, Universidad de San Martín de Porres]. https://hdl.handle.net/20.500.12727/609

Carbajal, J. (2013). *Definición de una metodología para la elaboración de auditorías de sistemas informáticos en entidades del Sistema Nacional de Control Peruano.* [Tesis maestría, Universidad de Piura]. https://hdl.handle.net/20.500.12727/609

Cazau, P. (2006). *Introducción a la investigación en ciencias sociales.*

Chicano, E. (2014). *Auditoría de seguridad informática.* IC Editorial.

Derrien, Y. (2009). *Técnicas de la auditoría informática.* Marcombo.

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método.* Ministerio de Hacienda y Administraciones Públicas.

Enríquez, E. (2013). OCTAVE, metodología para el análisis de riesgos de TI. *Universo: Periódico de los Universitarios,* 5-7.

Escrivá, G., y Romero, R. (2013). *Seguridad informática*. Macmillan Iberia, S.A.

Fontecha, D. (2014, diciembre 08). *Metodologías para el análisis de riesgos.* https://acortar.link/xBCv1v

García, M. (1992). *El análisis de la realidad social: Métodos y técnicas de investigación.* Alianza Universidad.

Giménez, J. (2014). Seguridad en equipos informáticos. IC Editorial.

Gutiérrez, C. (2013, mayo 14). *MAGERIT: metodología práctica para gestionar riesgos*. https://acortar.link/DclMuU

Hernández, R. (2016). *Metodología de la Investigación.* 4th ed. Mc Graw Hill.

Huerta, A. (2012, abril 02). Introducción al análisis de riesgos – Metodologías (II) [Internet]. *Security Art Work.* https://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-–-metodologias-ii/

Jiménez, J. (2009). *Evaluación: seguridad de un sistema de información.* El Cid Editor.

Kerlinger, F. (2002). *Enfoque Conceptual de la Investigación del Conocimiento.* Editorial Interamericana.

Lapiedra, R., Devece, C., and Guiral, J. (2011). *Introducción a la gestión de sistemas de información en la empresa.* Universitat Jaume I. Servei de Comunicació i Publicacions.

Marchand, W. (2013). *Metodología de implantación del modelo Balanced Scorecard para la gestión estratégica de TIC. Caso: Universidad Nacional Agraria de la Selva*. [Tesis maestría, Universidad de Piura]. https://pirhua.udep.edu.pe/handle/11042/1842

Molina, M. (2015). *Propuesta de un plan de gestión de riesgos de tecnología aplicado en la Escuela Superior Politécnica del Litoral.* [Tesis licenciatura, Universidad Politécnica de Madrid]

More Reaño, R.E. (2017). *Metodologías de evaluación de riesgos. Informáticos para mejorar la seguridad del área de sistemas de la unidad de gestión educativa local Sullana – Piura, 2016.* [Tesis de maestría, Universidad Católica Los Ángeles Chimbote]. https://hdl.handle.net/20.500.13032/15326

Namakforoosh, M. (2005). *Metodología de la Investigación.* (Segunda Edicion ed.) Limusa.

Peso, E., y Ramos, M. (2015). *La seguridad de los datos de carácter personal* (2a. ed.). Ediciones Díaz de Santos.

Pita, S., y Pertégas, S. (2002). Investigación cuantitativa y cualitativa. *Cadernos de atención primaria, 9*(2), 76-78

Plasencia, J. (2013). Nivel de gestión de la adquisición e implementación de las Tecnologías de Información y Comunicaciones (TIC) en la municipalidad provincial del Santa, departamento de Ancash en el Año 2016. [Tesis pregrado, Universidad Católica Los Ángeles de Chimbote]. https://hdl.handle.net/20.500.13032/33042

Sosa, H. (2017). *Análisis de Riesgos.*

UGEL Sullana. (s.f.). *Unidad de Gestión Educativa Local.* https://www.gob.pe/ugelsullana

Villena Aguilar, M. (2006). *Sistema de gestión de seguridad de información para una institución financiera.* [Tesis pregrado, Pontificia Universidad Católica del Perú]. http://hdl.handle.net/20.500.12404/362


ATIK
editorial

ATIK
editorial

Amenaza, riesgo y respuesta

Metodologías de evaluación de riesgos informáticos

ISBN: 978-9942-7145-0-3